

普通高等学校本科专业设置申请表

校长签字：

马宇

学校名称（盖章）：电子科技大学成都学院

学校主管部门：四川省

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-17

专业负责人：彭光辉

联系电话：15378205217

教育部制

1. 学校基本情况

学校名称	电子科技大学成都学院	学校代码	13665
主管部门	四川省	学校网址	http://www.cdustc.cn/
学校所在省市区	四川成都四川省成都市 高新西区百叶路	邮政编码	611731
学校办学基本类型	☐ 教育部直属院校 ☐ 其他部委所属院校 ☒ 地方院校 ☐ 公办 ☒ 民办 ☐ 中外合作办学机构		
已有专业学科门类	☐ 哲学 ☒ 经济学 ☐ 法学 ☒ 教育学 ☒ 文学 ☐ 历史学 ☒ 理学 ☒ 工学 ☐ 农学 ☐ 医学 ☒ 管理学 ☒ 艺术学		
学校性质	☒ 综合 ☐ 理工 ☐ 农业 ☐ 林业 ☐ 医药 ☐ 师范 ☐ 语言 ☐ 财经 ☐ 政法 ☐ 体育 ☐ 艺术 ☐ 民族		
曾用名	电子科技大学国腾软件学院 电子科技大学国腾学院		
建校时间	2001	首次举办本科教育年份	2001年
通过教育部本科教学评估类型	尚未通过本科教学评估	通过时间	-
专任教师总数	1016	专任教师中副教授及以上职称教师数	454
现有本科专业数	38	上一年度全校本科招生人数	4160
上一年度全校本科毕业生人数	3295		
学校简要历史沿革	2001年由电子科技大学与成都国腾实业集团合作创办的独立学院，以本科层次为主的普通高等学校。现有8个学院，76个专业，在校学生18000余名。学校现有成都和什邡两个校区，占地1400亩。学校先后荣获“四川省人才开发先进单位”、“全国教育系统先进集体”、“全国先进独立学院”等荣誉称号。		
学校近五年专业增设、停招、撤并情况	2021-2025年，学校共增设本科专业3个，有5个本科专业有停招情况，撤销4个本科专业。		

2. 申报专业基本情况

申报类型	新增国控专业
------	--------

专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	计算机学院网络空间安全系		
学校现有相近专业情况			
相近专业1专业名称	信息安全（注：可授理学、工学或管理学学士学位）	开设年份	2017年
相近专业2专业名称	网络工程	开设年份	2004年
相近专业3专业名称	-	开设年份	-

3. 申报专业人才需求情况

申报专业主要就业领域	主要就业方向可归纳为以下五大领域： 1. 政府与公共安全领域 岗位方向：网络安全监管、电子政务安全运维、应急响应处置。 核心职责：监测网络攻击事件、制定安全策略、保障政务系统（如“一网通办”）稳定运行。 2. 金融、能源、汽车等关键基础设施行业 岗位方向：金融风控安全、能源系统防护、数据隐私保护。 核心职责：防范DDoS攻击、交易欺诈检测、工业控制系统（ICS）安全加固。 3. 互联网与科技企业 岗位方向：安全产品研发、渗透测试、云安全运维。 核心职责：开发下一代防火墙、漏洞挖掘、保障云平台（如AWS、阿里云）租户数据隔离。 4. 咨询与合规服务 岗位方向：等保测评、GDPR合规审计、安全战略咨询。 核心职责：为企业提供等保2.0三级认证辅导、跨境数据传输合规方案设计。 5. 科研与教育机构 岗位方向：安全技术研究、密码学算法设计、高校教学。
------------	--

	核心职责：突破后量子密码（PQC）技术、开发AI驱动的自动化防御工具、培养下一代安全人才。	
人才需求情况	在数字化浪潮下，网络空间安全人才需求呈现爆发式增长。从国家战略层面看，网络强国战略与总体国家安全观强调网络安全核心地位，要求构建坚实的网络安全防线，这离不开大量专业人才支撑。 行业现状方面，据教育部预测，到2027年我国网络安全人员缺口将达327万。随着各行业数字化转型加速，金融、能源、交通等关键领域对网络安全保障需求激增，企业急需专业人员应对网络攻击、数据泄露等风险。 政策推动进一步加剧人才需求。国家将网络空间安全设为一级学科，鼓励高校与企业产教融合，共建网络安全学院和实验室。同时，在产业政策上给予大力支持，吸引更多资源投入网络安全领域，也带动了对专业人才的需求。在此背景下，培养兼具扎实专业知识、丰富实践经验和创新能力的网络空间安全人才，成为满足行业发展需求、保障国家网络安全的关键。 从我院合作用人单位方面，目前计算机分院对口的网络安全合作企业有天融信、奇安信、工业信息安全（四川）创新中心、国信安产业基地、亚信安全、安恒信息技术有限公司等多家龙头企业、其中和安恒信息技术有限公司建立了校内外实训基地、奇安信企业为我们提供了“网神安全”实训系统，目前正在和西部预备役大队接洽，合作企业范围覆盖国企、军工、私有龙头。 在相关企业的调研中，各个企业对本校开设网络空间安全专业表示积极的支持，从企业用人的角度共同帮助我们制定培养方案，其中天融信需要网络渗透、网络测试等方面的人才；奇安信需要安全逆向、网络安全运维、网络渗透等方面人才；国信安和亚信安全对具体方面没有具体指明，但表示网络空间安全专业的所有学生都是他们的招聘目标。	
申报专业人才需求调研情况	年度招生人数	80
	预计升学人数	5
	预计就业人数	75
	成都创信华通信息技术有限公司	5
	国信安产业基地	10
	亚信安全	15
	安恒信息技术有限公司	20
	奇安信科技有限公司	25

4. 产业调研报告

产业调研报告

一、引言

随着信息技术的飞速发展和网络空间的不断拓展，网络空间安全已成为国家安全的重要组成部分。为应对日益严峻的网络安全挑战，培养高素质的网络空间安全专业人才显得尤为重要。本报告基于《中国网络安全产业分析报告（2024年）》及其他相关数据，对新增网络空间安全本科专业的行业背景、市场需求、技术发展趋势及人才培养等方面进行深入调研与分析。

二、行业背景与政策环境

1. 行业背景

网络安全是保障网络系统硬件、软件及数据安全的关键领域，其核心目标是维护网络环境的可用性、完整性与保密性。随着数字化转型加速，网络安全已上升至国家安全、社会稳定和经济发展的战略高度。

全球网络安全市场规模持续扩张，2024年已达数千亿美元，预计2025年在中国市场将接近千亿元规模。这一增长主要得益于三大动力：一是政企数字化转型推动云安全、物联网安全需求激增；二是政策法规密集出台，如中国的《网络安全法》《数据安全法》及等保2.0等，强制要求企业强化安全建设；三是新兴技术融合带来复杂挑战，5G、AI、区块链等技术普及催生新型攻击手段，倒逼安全防护技术迭代。

技术层面，AI与量子计算正重塑行业格局。AI在攻防两端深度应用，既提升漏洞挖掘效率，也加剧自动化攻击威胁；量子计算则对传统加密体系构成潜在风险，推动后量子密码（PQC）与量子密钥分发（QKD）研究加速。此外，零信任架构逐步取代传统边界防护，成为金融、政府等关键领域的主流安全模型。

政策监管方面，全球主要经济体均加强网络安全立法。中国构建了以“四法一条例”为核心的法律框架，并强化数据跨境流动监管；欧美则通过NIST标准化、GDPR等规则推动全球网络空间治理。

当前，行业面临头部企业竞争加剧、技术同质化、人才短缺等挑战，但智能汽车、低空飞行器等新兴场景，以及“一带一路”国际化布局，仍为行业提供广阔增长空间。未来，网络安全企业需聚焦AI、量子安全等前沿技术，深化政企合作，同时拓展全球化服务能力，以应对日益复杂的网络威胁。

2. 政策环境

近年来，随着地缘政治不稳定不确定因素日益增多，技术发展日新月异，全球各国不断加强网络弹性建设，通过加强立法、技术创新和国际合作等手段加速网络安全战略布局，80%以上的国家颁布网络安全法规政策，140多个国家设立了网络安全事务协调机构，110多个国家出台个人数据与隐私保护法规，60%以上的国家通过外资审查、市场许可证等方式管理网络安全产品准入，以应对不断演变的网络安全挑战。2023年下半年以来，美国相继发布《2023年网络战略》《2024财年国防授权法案》《关键与新兴技术清单（2024年更新版）》《国际盟友合作伙伴标准指南》《2023年网络安全监管协调草案》《网络访问安全的现代方法》《供应链网络安全原则》等法规政策，从加强网络安全资金支持、促进关键技术研发、保障供应链网络安全、联合盟友强化战略合作等方面提出更加全面细化的措施要求；欧盟陆续推出《欧盟网络安全条例》《网络弹性法案》，针对数字产品、工业网络等领域规定了更加完备、更具约束力的网络安全要求和治理框架。全球主要国家和地区持续优化网络安全战略布局，为我国洞察和把握全球网络安全形势变化、强化我国网络安全产业顶层治理提供参考。我国政府高度重视网络安全工作，将网络安全纳入国家安全战略，出台了一系列政策法规以推动行业发展。

我国已构建起较为完善的网络安全政策法规体系，包括《未成年人网络保护条例》《中华人民共和国保守国家秘密法》《网络安全法》《数据安全法》《个人信息保护法》等，为网络安全产业的发展提供了坚实的法律保障。《网络数据安全条例（草案）》审议通过，作为行政法规对《网络安全法》《数据安全法》和《个人信息保护法》等上位法的有关规定进行落实、细化、补充，将对网络数据实行分类分级保护，明确各类主体责任，落实网络数据安全保障措施。政策方面，围绕数字政府、数据资产管理、数据安全、数据要素、数据跨境流通、关键信息基础设施安全保护、安全应急预案等方面发布系列政策规定，同时在工业和信息化领域、新兴技术、寄递服务、民用航空、保险、电力系统、教育行业等细分应用领域提出网络安全和数据安全管理要求。可以看到，我国网络安全政策立法总体呈现不断优化调整、细化落实现有政法体系的趋势，同时紧跟新兴技术发展伴随的网络防御新特点新形势，提出具有前瞻性、突破性的网络安全治理理念，更加多元、审慎的政法体系为网络安全产业健康有序发展营造了良好环境。同时，政府还通过税收优惠、资金支持、人才培养等多种政策措施，鼓励企业加大网络安全技术研发和人才培养投入，推动行业快速发展。

三、市场需求分析

1. 市场规模持续增长

受益于网络安全政策加码以及新技术、新业态安全需求不断释放，全球网络安全产业逐步复苏回暖，网络安全企业积极加强业务布局，加速技术迭代创新，人工智能、零信任、量子信息等前沿技术为网络安全产业发展注入新活力，从供需两侧促进全球网络安全投入持续增长，全球网络安全产业发展长期向好的基本面没有改变。

根据《中国网络安全产业分析报告（2024 年）》，全球网络安全市场支出不断攀升。据 Gartner 统计预测数据显示，2019 年至 2024 年全球网络安全支出同比增速呈现上升趋势，预计 2024 年将达到 2149.5 亿美元，同比增长 14.3%（见图 4.1），全球网络安全需求仍然强劲。细分领域看，安全服务、基础设施保护、网络安全设备支出占比最高，2024 年将分别达到 41.9%、15.5%、11.3%。

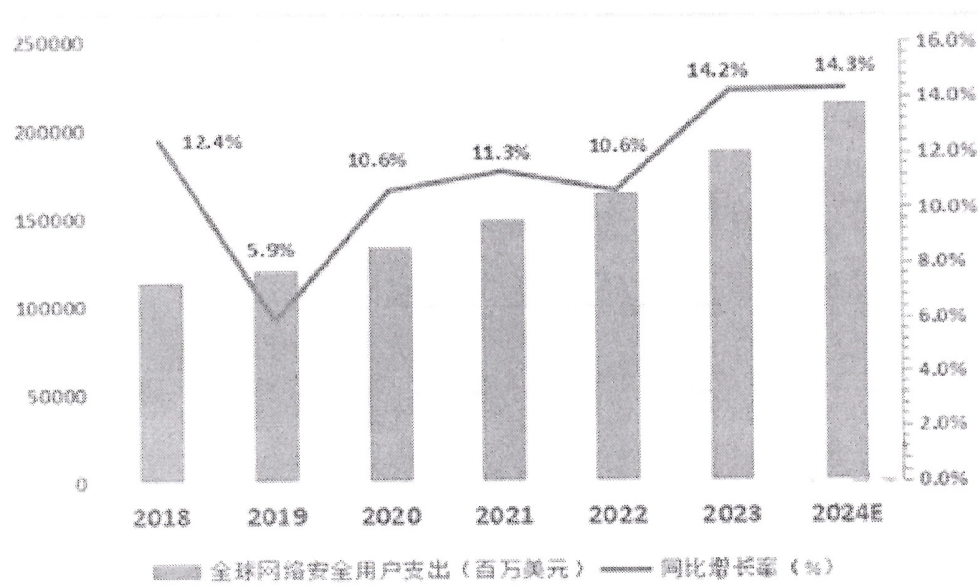


图 4.1 2018—2024 年全球网络安全支出及同比增长率

根据世界经济论坛（WEF）与埃森哲联合发布的《2024 年全球网络安全展望》，2023 年，全球网络安全经济的增长速度达到世界经济增速的 4 倍；据全球市场调研机构 MarketsandMarkets 预计，全球网络安全市场规模预计将从 2023 年的 2200 亿美元增长到 2027 年的 2662 亿美元，年复合增长率（CAGR）达 3.9%。



图 4.2 2023 年中国网络安全市场规模及增速

2023 年中国网络安全市场规模及增速如图 4.2 所示，2023 年中国网络安全市场规模达到约 640 亿元，同比增长 1.1%。尽管增速较 2022 年有所下降，但市场规模依然保持增长态势。预计到 2026 年，我国网络安全市场规模将超过 800 亿元，展现出强劲的增长潜力。

2. 行业需求多样化

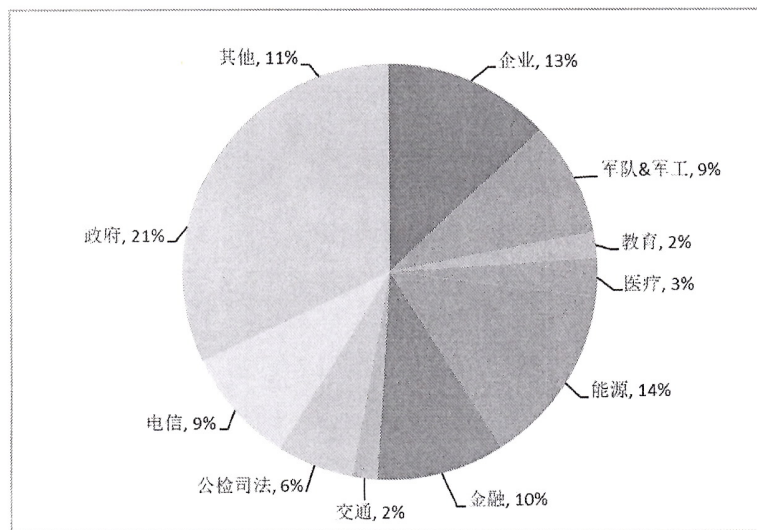


图 4.3 2023 年中国网络安全项目数量行业分布

从网络安全客户所属行业分布来看，政府部门因政策监管严格，其信息系统涉及国计民生和国家安全等重要业务，中国网络安全产业联盟（CCIA）对网络安全项目的需求较大，近年来一直占据最大份额；能源、企业、金融、电信、军工、公检法司、医疗、交通、教育等与国计民生紧密相关的领域紧

随其后，作为密集数据源生产、持有和使用方，网络安全需求和投入均十分可观（见图 3）。

3. 人才缺口巨大

根据重点企业调研数据，2023 年国内百家网络安全主要企业的从业人员数量达 91798 人，据教育部数据显示，到 2027 年，我国网络安全人员缺口将达 327 万人。网络安全相关本科专业毕业生规模有限，远不能满足市场需求。特别是在中小型企业中，由于数字化转型的加速推进，网络安全人才需求更加旺盛。

四、技术发展趋势

1. 人工智能与机器学习

人工智能和机器学习技术在网络安全领域的应用日益广泛，能够自动识别和防御复杂的安全威胁，提高安全运营效率。“人工智能+安全”技术将实现对网络攻击及威胁的“免疫性防御”，成为未来网络安全发展的重要方向。

2. 量子加密通信技术

量子加密通信技术利用量子不可分割、量子态不可克隆等特性，实现绝对安全的信息传输和密钥分发。随着量子计算技术的发展，量子加密通信技术将在国防军工、电子政务、金融证券等领域发挥重要作用。

3. 隐私增强技术

隐私增强技术通过硬件或软件的可信执行环境、安全多方计算、差分隐私等手段，保护个人数据隐私。随着数据保护法规的加强，隐私增强技术将在政务、金融、医疗等领域得到广泛应用。

4. 持续威胁暴露管理

持续威胁暴露管理技术通过动态监控和管理潜在攻击，增强组织整体安全防御能力。该技术将成为企业安全管理能力的建设重点，推动网络安全防御向主动防御转变。

五、就业前景

（一）市场需求情况

1. 人才缺口持续扩大

缺口规模：预计到 2027 年，我国网络安全人才缺口将达 327 万人。

网络安全运营：占比最高的岗位（29.4%），涵盖安全监控、应急响应等。

数据安全：随着《数据安全法》实施，需求激增，岗位多要求高（如加密技术、隐私保护）。

新兴领域：AI 安全、物联网安全、低空经济安全（如无人机防御）成为新增长点。

2. 行业区域急需

核心区域：华北（31%）、华东（26%）、华南（14%）为需求集中地，一线城市薪资水平领先。

企业类型：政府/国企、金融、电力、通信、互联网为五大需求行业，中小型企业数字化转型催生大量岗位。

3. 用人标准

技能优先：实战能力（如渗透测试、漏洞利用）和证书（CISP/CISSP）成为“硬通货”。

年轻化趋势：30 岁以下从业者占比超 60%，需适应高强度学习与快速迭代的技术。

（二）职业发展路径

网络安全专业毕业生凭借其技术深度和行业需求，职业路径呈现多元化且晋升空间广阔的特点。以下是典型职业路径的详细描述，涵盖技术、管理、合规与创业四大方向，如表 4.1 所示：

表 4.1 网络安全专业职业发展路径

方向	时间线	岗位职责	技能要求
技术路线：从安全工程师到架构师/专家	初级安全工程师（1-3 年）	负责基础安全运维，如漏洞扫描、日志分析、防火墙配置；参与渗透测试、代码审计等安全评估工作。典型岗位：安全运维工程师、渗透测试工程师、代码安全工程师。	熟悉常见安全工具（如 Nmap、Wireshark、Burp Suite）；掌握基础编程（Python/Shell）和操作系统原理。
	中级安全工程师 /	主导复杂安全项目，如 APT 攻击溯源、数据泄露调查；设计安全	精通攻防技术（如 Web 安全、二进制漏洞挖

	安全分析师（3-5年）	解决方案（如零信任架构、SDP）；参与安全研发，如开发安全工具或平台。典型岗位：高级渗透测试工程师、安全研发工程师、威胁情报分析师。	掘）；具备威胁情报分析能力；熟悉云安全（AWS/Azure/阿里云安全配置）。
	高级安全架构师 / 安全专家（5-10年）	规划企业整体安全战略，设计安全体系架构（如数据加密、身份认证）；主导重大安全事件应急响应；推动安全技术创新（如AI安全、量子安全）。典型岗位：首席安全官（CSO）、安全架构师、安全顾问。	深度理解业务安全需求；具备跨领域技术整合能力（如安全与DevOps结合）；持有CISSSP、CISP-PTE等高级认证。
管理路线：从项目经理到部门负责人	安全项目经理（3-5年）	管理安全项目全生命周期，包括需求分析、资源协调、进度监控；确保项目符合合规要求（如等保2.0、GDPR）。	项目管理能力（PMP认证）；熟悉安全标准（ISO 27001、NIST CSF）；具备跨部门沟通能力。
	安全团队主管（5-8年）	领导安全团队（如SOC、红队、蓝队），制定团队目标与KPI；优化安全流程（如SDL、DevSecOps）；培养团队技术能力。	团队管理能力；战略思维；熟悉行业趋势（如SASE、XDR）。
	安全部门负责人 / CSO（8年以上）	制定企业安全战略，与董事会、监管机构沟通；管理安全预算与资源分配；推动安全文化落地。	企业级安全视野；商业敏感度；领导力与影响力。
合规与咨询路线：从合规专员到安全合规专家	合规专员（1-3年）	协助企业满足法规要求（如《网络安全法》《数据安全法》）；整理合规文档（如等保测评报告、隐私政策）。	熟悉法律法规；具备文档撰写能力；了解基础安全技术。
	合规分析	为企业提供合规解决方案（如跨	深入理解行业合规标

	师 / 咨 询 顾 问（3-5 年）	境数据传输合规）；设计安全合 规框架（如 GDPR 合规体系）； 参与安全审计与认证。	准（如 HIPAA、PCI DSS）；项目咨询能力； 跨文化沟通能力（针对 跨国企业）。
	首席合规 官（CCO） / 安 全 合 规专家（8 年以上）	领导企业合规战略，与监管机构 保持沟通；管理全球合规项目； 应对重大合规风险（如数据泄露 调查）。	法律与商业复合背景； 危机管理能力；国际视 野。
创业路线：从 技术创始人 到安全企业 领导者	技术创始 人（3-5 年 经验后）	安全服务：渗透测试、红队演练、 应急响应。 安全产品：开发下一代防火墙、 EDR、SOAR 平台。 安全培训：CTF 竞赛、企业内训、 认证考试辅导。	技术创新能力；商业敏 锐度；资源整合能力 （如融资、团队搭建）。
	安全企业 CEO/CTO （ 5-10 年）	制定企业战略，拓展市场与客 户；管理产品研发与交付；维护 投资者与合作伙伴关系。如奇安 信创始人齐向东、启明星辰创始 人严立，均从技术背景转型为企业 领导者。	战略规划与决策能力； 资源整合与资本运作 能力；客户需求洞察能 力、跨行业资源链能 力；接品牌影响力塑造 能力。

（三）行业趋势与职业机遇

新兴领域：AI 安全、量子安全、车联网安全、低空飞行器安全。

全球化需求：随着“一带一路”推进，中国网络安全企业加速出海，需具备跨文化安全服务能力。

政策红利：数据安全法、关键信息基础设施保护条例等法规推动合规需求爆发。

六、人才培养与专业建设

（一）政策驱动与战略定位：国家需求引领人才培养方向

1、顶层设计强化

网络安全已被提升至国家战略高度，2025 年相关政策体系持续完善：

法律法规：《网络安全法》《数据安全法》《个人信息保护法》等明确要求关键信息基础设施运营者定期开展网络安全教育培训，推动行业人才需求激增。

学科建设：全国 56 所高校设立网络安全学院，形成“本硕博”完整培养链条，2025 年相关专业在校生规模预计达 3.5 万人。

专项支持：中央财政设立 10 亿元专项基金，用于学科建设、高端人才引进及国际学术交流，为人才培养提供资金保障。

2、产业需求倒逼改革

人才缺口巨大：据国家网信办数据，2025 年行业人才缺口达 200 万人，较 2023 年增长 33%。高端实战型人才（如国家级攻防专家）不足 5000 人，中西部省份每万人安全人才密度不足东部地区的 1/3。

新兴领域紧缺：AI 安全、量子安全、隐私计算等前沿领域专业人才供给量不足市场需求的 5%，金融行业 AI 安全架构师年薪普遍突破 80 万元。

政策驱动型需求激增：数据分类分级管理、跨境数据合规等细分领域新增人才需求超 50 万人，信创工程推动下，掌握国产操作系统安全适配技术的工程师需求年增幅达 300%。

（二）高校网络空间安全专业现状

1、专业开设高校数量

截至 2024 年 6 月，全国共有 626 所高校开设网络空间安全相关专业，覆盖普通高校总数的 21.8%。其中，本科院校 283 所，高职院校 343 所 25。河南、山东、四川、江苏、湖北等省份开设院校数量居前 11。

2、细分专业分布

网络空间安全专业覆盖以下细分方向（截至 2024 年 9 月）：网络空间安全专业 43 所高校开设；信息安全专业 139 所高校开设；信息对抗技术专业 21 所高校开设；网络安全与执法专业 26 所高校开设；密码科学与技术专业 20 所高校开设。

3、毕业生规模与人才缺口

年毕业人数：网络安全相关专业（含细分方向）年毕业生超 2 万人。但网络安全相关本科专业（信息安全、网络空间安全、网络安全与执法）的年毕业生规模仅约 1.45 万人。

人才供需矛盾：当前培养规模远低于市场需求，到 2027 年全国网络安全人员缺口将达 327 万。中小型企业数字化转型加速，网络安全运营岗位需求占比高达 29.4%，加剧人才短缺。

4、学科建设进展

学科体系：34 所高校设立“网络空间安全”一级学科（代码 0839），授予工学学位。

学院设置：超 90 所高校成立专门网络空间安全学院（如北航、西电、武大等），其余高校多在计算机学院、信息学院下设该专业。

（三）高校专业建设：课程体系迭代与产教融合深化

1、课程体系前沿化

核心课程升级：全国高校普遍将《后量子密码学》《数据跨境流动合规实务》等前沿课程纳入培养方案，覆盖密码学、区块链、AI 安全等新兴技术。

交叉学科融合：如东南大学开设“网络空间安全+法学”双学士学位项目，武汉大学构建“计算机+法学+心理学”多学科课程体系，培养复合型人才。

实践平台拓展：360、深信服等企业 with 高校共建 200 余个实训基地，推动“产学研用”深度融合。例如，广西科技大学师生构建的“广西教育系统安全数字化支撑平台”已突破多项关键技术。

2、产教融合模式创新

联合培养基地：天融信与北京邮电大学共建的《校企产学研深度协同的网络空间安全实战人才联合培养基地》，通过课题研究、专业建设、实习实训三个维度深化合作，学生参与企业真实项目，产出专利、代码原型等成果 50 余件。

双导师制推广：各地政府联合龙头企业建设 100 个现代产业学院，企业技术骨干与高校教授共同指导实践课程，定向输送实战型人才。例如，青岛科技大学与英科医疗合作设立“定向培养班”，学生需完成企业真实需求项

目方可毕业。

竞赛驱动能力提升：齐鲁师范学院通过“学科竞赛+行业竞赛+攻防演练”三级竞赛体系，近三年获省部级以上奖励 100 余项，学生实战能力显著增强。

（四）区域协同与资源整合：破解“东强西弱”格局

1、地方院校差异化发展

中西部高校崛起：广西科技大学依托“广西教育系统网络安全监测中心”，承担全区 106 所高校网络安全监测任务，累计发现并整改安全风险 4000 余个，形成“服务区域、辐射全国”的特色模式。

校际联动机制：广西科技大学牵头建立院校联盟，与河池学院等 10 余所院校共享课程资源，实现“专本联动”“本硕衔接”，破解单一院校资源不足问题。

政企行协同育人：甘肃政法大学与甘肃省公安部门合作，教师被聘为“网络攻防专家库专家”，为学生提供真实案件分析素材；南昌大学联合中国网络安全审查技术与认证中心（CCRC），将行业认证纳入课程体系，学生毕业时可同步获得 CISP 认证资格。

2、资源共享与生态共建

东西部人才共享机制：在西安、成都等地建设“网络安全飞地园区”，鼓励东部人才以项目制、顾问制等方式参与西部建设，缓解区域资源错配问题。

科研成果转化：广西科技大学突破的“端边云协作数据安全技术”已应用于东盟安保项目，累计发现 23 家单位 47 个安全风险，推动区域安全生态完善。

社会服务能力提升：齐鲁师范学院学生开发的“网络安全能力画像大数据分析平台”被山东省教育厅采纳，用于全省高校安全评估，体现高校对区域安全的支撑作用。

（五）挑战与未来方向：构建“金字塔型”人才体系

1、核心挑战

供应链安全风险：关键技术领域人才储备不足，如抗量子密码领域专业人才年增幅需达 40%才能满足需求。

高端人才流失：核心团队稳定性面临考验，需通过政策杠杆（如税收优

惠、住房补贴）提升人才留存率。

区域失衡加剧：京津冀、长三角、粤港澳大湾区集中了全国 70%的安全人才，中西部省份需通过“飞地经济”“校际联盟”等模式突破人才虹吸效应。

2、未来路径

塔尖引领：选拔 500 名“网络安全战略科学家”，依托国家实验室、重点科研项目开展攻关，给予长期稳定支持。

塔身支撑：通过“蓝军训练营”“全国网络安全大赛”等实战平台，每年培养 10 万名具备渗透测试、应急响应能力的实战型工程师。

塔基夯实：实施“全民安全意识提升工程”，三年内完成 1000 万人次的政企员工安全培训，构建全社会网络安全防护意识防线。

国际化布局：山东大学、西安电子科技大学等高校与海外名校联合开设“网络空间国际治理”交叉学科，每年输送百余名复合型人才参与全球规则博弈。

七、结论与展望

1、结论

在数字化与地缘政治博弈交织的背景下，网络空间安全已成为国家安全、社会稳定与经济基石。增设网络空间安全专业，既是响应国家战略需求、填补人才缺口的必然选择，也是顺应技术变革、抢占产业制高点的关键举措。通过构建“政产学研用”协同育人体系，培养具备 AI 安全、车联网安全、量子安全等前沿能力的复合型人才，培养具有动手实践能力强综合素质高的复合型人才，将为我国网络安全产业高质量发展提供核心支撑。

2、展望

未来，随着数字化转型的加速推进和新兴技术的发展应用，网络空间安全领域将迎来更加广阔的发展前景。新增网络空间安全本科专业将为我国网络安全产业的发展注入新的活力，为保障国家网络信息安全作出重要贡献。同时，我们也需要关注行业发展趋势和技术创新动态，不断调整和优化专业设置和人才培养方案，以适应行业发展的需求。

5. 申请增设专业人才培养方案

网络空间安全专业培养方案

一、专业名称及专业代码

专业名称：网络空间安全专业

专业代码：080911TK

二、学制及授予学位名称

学制：四年

授予学位：工学

学生修满教学计划规定的最低学分，达到毕业要求，且符合学位授予的有关规定，可向校学位委员会提出学位申请，经校学位委员会审定合格后授予工学学士学位。

三、培养目标

本专业培养素质、知识、能力全面发展，具有自然科学、人文科学和信息科学技术基础知识，掌握网络空间安全领域基本理论、基本技术和基本应用，具备网络空间安全技术开发和应用服务工作能力的应用型高素质人才。具体体现在：

培养目标 1：培养具有坚实网络安全专业理论知识、健全的人格和良好的人文素养，在网络安全工程实践中能遵守职业道德和规范，具有服务社会的意愿和能力。

培养目标 2：培养具备较强的网络空间安全创新能力和工程实施能力，能在企事业单位、政府部门和教育行业及相关领域，作为技术骨干承担网络安全方面的技术研究、项目管理、分析设计和运行维护等工作的应用型人才。

培养目标 3：培养具有良好的沟通协作和团队管理能力，能够在多学科环境中参与或领导团队有效实施安全系统项目。

培养目标 4：具备自主学习和适应发展的能力，能够通过多种途径持续学习，掌握网络空间安全领域国内外前沿动态和行业需求发展变化。

四、毕业要求

本专业学生经过培养和训练后，毕业生在知识、能力、素质方面应达到以下要求：

1. 工程知识：能够将数学、自然科学、工程基础和专业知识用于解决复

杂网络空间安全工程问题。

2. 问题分析：能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析复杂网络空间安全工程问题，以获得有效结论。

3. 设计/开发解决方案：能够设计针对复杂网络空间安全工程问题的解决方案，设计满足特定需求的系统、单元（部件）或工艺流程，并能够在设计环节中体现创新意识，考虑社会、健康、安全、法律、文化以及环境等因素。

4. 研究：能够基于科学原理并采用科学方法对复杂工程网络安全问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论。

5. 使用现代工具：能够针对复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息工具，包括对复杂工程网络安全问题的预测与模拟，并能够理解其局限性。

6. 工程与社会：能够基于工程相关背景知识进行网络安全合理分析，评价专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。

7. 环境和可持续发展：能够理解和评价针对复杂工程网络安全问题的专业工程实践对环境、社会可持续发展的影响。

8. 职业规范：具有人文社会科学素养、社会责任感、爱国意识，能够在网络安全工程实践中理解并遵守网络安全职业道德和规范，履行责任。

9. 个人和团队：能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。

10. 沟通：能够就复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令。并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

11. 项目管理：理解并掌握工程管理原理与经济决策方法，并能在多学科环境中应用。

12. 终身学习：具有自主学习和终身学习的意识，有不断学习和适应发展的能力。

五、主要课程

专业主干课程主要用于构建学生将基本原理与技术运用于信息安全科学研究、技术开发和应用服务等工作能力。教学内容主要包含信息科学基础、信息安全基础、网络攻防等知识领域的基本内容，主要分为学科基础课程、专业必修课程、专业选修课程三类。具体相应的课程请参考专业方向课程培养路线图。

学科基础课程

C 程序设计、数据结构与算法基础、计算机组成与系统结构、信息安全数学基础、数据库原理及安全、python 程序设计与应用实战、计算机网络、操作系统原理及安全。

其中，操作系统原理与安全的主要任务是训练学生能灵活运用当今主流的操作系统构建网络环境、进行网络管理、搭建各种网络服务、不同平台下的软件开发及移植的能力，培养学生综合运用所学知识进行综合实践的能力，最终让学生提高分析问题、并运用计算机技能解决实际问题的能力。

其中，数据库原理与安全旨在使学生系统地掌握数据库系统的基本原理和基本技术。要求在掌握数据库系统基本概念的基础上，能熟练使用 SQL 语言完成相应的要求；掌握数据库设计方法和步骤，具有设计数据库模式以及开发数据库应用系统的基本能力。

专业必修课程

网络空间治理、网络空间安全智能决策、汇编语言、网络攻击与防御、认知域对抗与防御、数据安全理论与实践、网络安全等级保护测评技术、代码安全审计、网络服务配置与管理、网络安全设备配置与管理。

网络空间治理课程聚焦网络空间行为规范与政策法规，涵盖国际网络治理框架（如联合国互联网治理论坛）、国家网络安全战略（如《网络安全法》《数据安全法》）、网络伦理与道德规范，以及跨境数据流动合规实务。培养具备法律素养与政策分析能力的复合型人才，能够制定企业数据合规方案、参与网络空间国际规则博弈，并胜任政府网络安全监管岗位。

网络空间安全智能决策课程融合 AI 与安全决策，包括威胁情报自动化分析、基于机器学习的攻击预测模型、安全事件应急响应智能调度系统。培养能够开发智能安全工具的工程师，如利用深度学习构建 APT 攻击检测系统，或设计基于强化学习的防火墙动态策略调整机制。学生需具备将安全需求转化为 AI 模型输入输出的能力。

汇编语言课程深入计算机底层架构，涵盖寄存器操作、内存寻址模式（如基址变址寻址）、中断处理机制，以及反汇编与逆向工程技术。培养具备系统级安全分析能力的“白帽黑客”，能够通过汇编代码审计发现软件漏洞（如缓冲区溢出）、分析恶意样本行为，并开发低级安全防护工具（如内核级 Rootkit 检测模块）。

网络攻击与防御课程实战化攻防技术体系，包括 Web 漏洞利用（SQL 注入、XSS）、二进制漏洞挖掘（堆溢出、UAF）、社会工程学攻击防御，以及红蓝对抗演练中的攻防策略制定。本课程旨在要求学生掌握各种漏洞原理的基础上，提高学生渗透测试能力及防御能力，为以后能从事相关安全工作打下良好的基础。例如，学生需掌握 Metasploit 框架定制化开发，针对工业控制系统设计专用攻击载荷。

认知域对抗与防御课程融合心理学与信息战，包括虚假信息传播模型构建、舆情情感分析算法、深度伪造（Deepfake）检测技术，以及认知域攻防演练平台设计。培养国家安全领域战略人才，能够识别境外势力网络认知战手段，开发反制宣传机器人，并设计基于区块链的舆情溯源系统。例如，学生需分析 Twitter 上 AI 生成的政治谣言传播路径，提出干预策略。

数据安全理论与实践课程涉及数据全生命周期防护，涵盖同态加密算法实现、联邦学习中的隐私保护机制、数据跨境流动安全评估框架，以及医疗、金融等敏感行业数据脱敏标准。培养数据安全治理专家，能够设计企业数据分类分级保护方案，并通过 ISO 27701 隐私信息管理体系认证。例如，学生需针对智能汽车采集的生物特征数据，制定加密存储与共享策略。

网络安全等级保护测评技术课程对等保 2.0 标准深度解析，包括云计算、物联网、工业控制系统等新型场景的测评方法，以及自动化测评工具开发（如基于 YARA 规则的恶意代码扫描）。培养等保测评师，能够独立完成三级等保系统测评报告，并指导企业通过等保认证。例如，学生需针对学校办公系统，设计符合等保要求的数据库审计方案。

代码安全审计课程通过静态与动态分析技术结合，包括 Fortify、Checkmarx 等工具使用，开源组件漏洞挖掘（如 Log4j2 远程代码执行漏洞），以及安全开发生命周期（SDL）实施。培养 DevSecOps 工程师，能够在 CI/CD 流水线中集成自动化安全测试，并开发自定义安全代码检查规则。

网络服务配置与管理课程通过对企业级网络服务部署，包括 DNSSEC 配置、HTTPS 证书生命周期管理、Kubernetes 集群安全加固，以及 SD-WAN 组网中的零信任接入控制。培养网络运维架构师，能够设计高可用、高安全的

网络服务架构，并通过 CISSP 认证。

网络安全设备配置与管理课程是通过对网络安全设备进行配置，实现下一代防火墙（NGFW）策略优化、SDN 环境下的安全资源动态调度、AI 赋能的入侵检测系统（IDS）调优，本课程也是网络安全等级保护测评技术的实施基础。本课程的教学目标一是学习网络安全设备原理与方法，二是掌握网络安全设备的配置与管理，三是为同学参与网络安全产品开发与网络安全服务工作打下基础。

专业选修课程

敏捷管理、信息论与编码、信息安全标准与法律法规、计算机等级保护与风险评估、网络安全应急响应、信息安全前沿科技、计算机病毒与防护技术。

其中，敏捷管理课程使学生能深刻理解敏捷管理的意义和概念，敏捷宣言，敏捷和传统瀑布模型的区别，以及敏捷代主流技术。重点介绍在敏捷体系中应用最为广泛的 scrum 敏捷管理。能够区分 scrum 的敏捷教练、产品负责人和开发团队角色的不同，并能够组建敏捷团队；熟练掌握 scrum 中的实施流程，如计划会议、每日站会、评审会议以及回顾会议的作用以及如何开展，熟练掌握产品列表、迭代列表、燃尽图等方法，熟练掌握一个 scrum 开发工具。

六、课程体系图

(1) 课程体系设置占比图

课程类别			最低毕业要求		
			学时	学分	学分比例
通识课程	通识必修课程	必修	1036	64	37.43%
	通识选修课程	选修	144	9	5.26%
学科基础课程		必修	240	15	8.78%
		基础实践	160	10	5.85%
专业课程	专业必修课程	必修	240	15	8.78%
		专业实践	256	16	9.34%
	专业选修课程	选修	160	10	5.85%
集中实践环节		必修	208	13	7.60%
		选修	304	19	11.11%
合计			2748	171	100.00%

图 5.1 课程体系设置占比图

网络空间安全专业课程体系设置包含通识课程、学科基础课程、专业课程、集中实践环节四部分，最低毕业要求总学时为 2748 学时，171 学分。课程设置占比图如图 5.1 所示。

(2) 网络空间安全课程体系图

网络空间安全课程体系从开设时间上分为 8 个学期，其中第一至四学期主要为通识课程、学科基础课程，第五、六学期主要为专业课程，第七、八学期主要为集中实践环节。具体课程体系安排如图 5.2 所示。

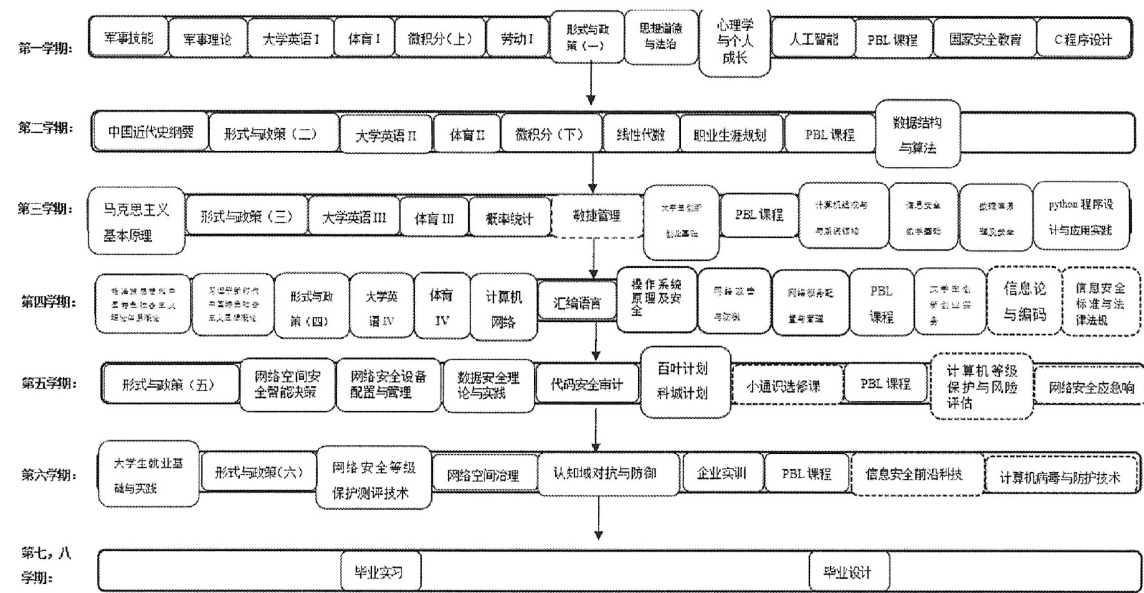


图 5.2 网络空间安全课程体系图

(3) 实践能力体系图

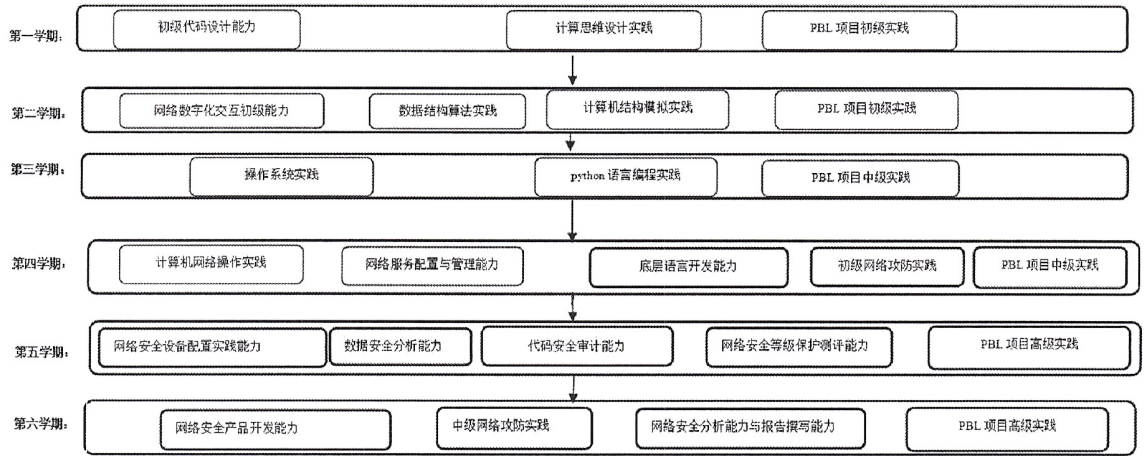


图 5.3 实践能力体系图

网络空间安全专业在第一至六学期授课时间段在课程中分别设置有相关课程的实践能力课程，以达到学以致用，以用促学，夯实基础的目的。具体实践能力设置如图 5.3 所示。

七、教学计划

网络空间安全专业教学计划共计 8 学期，课程类别包含通识课程、学科基础课程、专业课程、集中实践环节，设计必修和选修两种课程性质，毕业最低总学分要求 171 学分，其中通识课程（必修课程 64 学分、选修课程最低 9 学分），学科基础课程 25 学分，专业课程（必修课程 31 学分、选修课程最低 10 学分），集中实践环节（实习实训 24 学分、毕业实习 1 学分、毕业设计 7 学分）。教学计划具体安排如表 5.1 教学计划表所示。

表 5.1 教学计划表

课程类别	课程性质	课程编号	课程名称	学分	总学时	学时分配		开课学期	周学时	备注
						理论	实验/实践			
通识必修课程	必修	A400101	思想道德与法治	3	48	32	16	1	3	
	必修	A400103	中国近现代史纲要	3	48	32	16	2	3	
	必修	A400105	毛泽东思想和中国特色社会主义理论体系概论	3	48	32	16	4	3	
	必修	A400115	习近平新时代中国特色社会主义思想概论	3	48	48		4	3	
	必修	A400107	马克思主义基本原理	3	48	32	16	3	3	
	必修	A400124	形势与政策（一）	0.5	8	8		1	4	
	必修	A400125	形势与政策（二）	0.5	8	8		2	4	
	必修	A400126	形势与政策（三）	0.25	4	4		3	4	
	必修	A400127	形势与政策（四）	0.25	4	4		4	4	
	必修	A400128	形势与政策（五）	0.25	4	4		5	4	
	必修	A400129	形势与政策（六）	0.25	4	4		6	4	
	必修	A400201	大学英语 I	4	64	64		1	4	
	必修	A400202	大学英语 II	4	64	64		2	4	
	必修	A400203	大学英语 III	4	64	64		3	4	
	必修	A400204	大学英语 IV	2	32	32		4	2	
	必修	A400310	微积分（上）	4	64	64		1	4	

	必修	A400311	微积分（下）	4	64	64		2	4	
	必修	A400313	线性代数	4	64	64		2	4	
	必修	A400315	概率统计	3	48	48		3	3	
	必修	A400401	体育 I	2	32	32		1	2	
	必修	A400402	体育 II	2	32	32		2	2	
	必修	A400403	体育 III	2	32	32		3	2	
	必修	A400404	体育 IV	2	32	32		4	2	
	必修	A400501	军事理论	2	36	36		1		
	必修	A400605	大学生就业基础与实践	1	16	16		6	1	
	必修	A400606	职业生涯规划	1	16	16		2	1	
	必修	A400603	大学生创新创业基础	0.5	8	8		3		
	必修	A400702	心理学与个人成长	2	32	16	16	1	2	
	必修	A400703	人工智能	2	32	16	16	1	2	
	必修	A400122	劳动 I	0.5	16	16		1	2	
	必修	A400503	国家安全教育	1	16	16		1	2	
	小计			64	1036	940	96			
通识选修课程	选修	A400130	美育课程	2	32	32		2-7	2	
	选修	A400116	四史教育	1	16	16		2-5	1	
	限定性选修	B400017	工科生的商业决策	2	32	32		2-7	2	
	限定性选修	B400013	理工生的文献检索与成果转换	2	32	32		2-7	2	
	选修	H400000	公共任选	2	32	32		2-5	2	
	小计			9	144	144				
	最低毕业学分要求			9						
学科基础课程	必修	D402105	C 程序设计	4	64	32	32	1	4	S
	必修	D402002	数据结构与算法基础	3	48	32	16	2	3	S
	必修	D402122	计算机组成与系统结构	3	48	32	16	3	3	S
	必修	D402121	信息安全数学基础	2	32	16	16	3	2	S
	必修	D402125	数据库原理及安全	3	48	32	16	3	3	S
	必修	D402124	python 程序设计与应用实战	3	48	32	16	3	3	S
	必修	D402096	计算机网络	4	64	32	32	4	4	S
	必修	D402123	操作系统原理及安全	3	48	32	16	4	3	S

	小计			25	400	240	160			
专业必修课程	必修		网络空间治理	2	32	16	16	6	2	I
	必修		网络空间安全智能决策	2	32	16	16	5	2	I
	必修		汇编语言	3	48	32	16	4	3	S
	必修		网络攻击与防御	4	64	32	32	4	4	C
	必修		认知域对抗与防御	4	64	32	32	6	4	I
	必修		网络安全设备配置与管理	4	64	32	32	5	4	C
	必修		数据安全理论与实践	3	48	16	32	5	3	I
	必修		网络安全等级保护测评技术	3	48	16	32	6	3	C
	必修		代码安全审计	3	48	16	32	5	3	C
	必修		网络服务配置与管理	3	48	32	16	4	3	C
	小计			31	496	240	256			
专业选修课程	选修	F402102	敏捷管理	2	32	16	16	3	2	S
	选修	F402225	信息论与编码	2	32	16	16	4	2	S
	选修	F402118	信息安全标准与法律法规	2	32	16	16	4	2	C
	选修	F402223	计算机等级保护与风险评估	2	32	16	16	5	2	C
	选修	F402122	网络安全应急响应	2	32	16	16	5	2	C
	选修	F402121	信息安全前沿科技	2	32	16	16	6	2	A
	选修	F402135	计算机病毒与防护技术	2	32	16	16	6	2	A
	小计			14	224	112	112			
	最低毕业学分要求			10						
集中实践环节	课程性质	课程编号	课程名称	学分	总学时	学时分配		开课学期	周学时	备注
实习实训	必修	A400502	军事技能	2	32		32	1		
	必修	A400801	百叶计划	1	16		16	1-7		
	必修	A400901	科成计划	1	16		16	1-6		
	必修	A400123	劳动 II	0.5	8		8	1-7		
	必修	A400604	大学生创新创业实务	0.5	8	8		4		
	限定	G402001	PBL 项目实践 1/7	1	16		16	1		

	选修		(静态网站项目开发)							
	限定选修	G402002	PBL 项目实践 2/7 (高级网站项目开发)	2	32		32	2		
	限定选修	G402018	PBL 项目实践 3/7 (全栈产品开发)	3	48		48	3		
	限定选修	G402010	PBL 项目实践 4/7 (实战项目开发)	4	64		64	4		
	限定选修	G402009	PBL 项目实践 5/7 (企业项目开发)	4	64		64	5		
	限定选修	G402013	PBL 项目实践 6/7 (企业项目开发)	3	48		48	6		
	限定选修	G402019	企业实训	1	16		16	6		
	限定选修		PBL 项目实践 7/7 企业实习(二选一)	1	16		16	7		
	小计			24	384	8	376			
毕业实习	必修	G40		1				7		
毕业设计(论文、项目制、课程设计)	必修	G40		7				7-8		
集中实践环节最低毕业学分要求				32						
最低毕业总学分要求				171						

培养方案制定人：彭光辉 培养方案审核人：毛敏 培养方案批准人：张明善

6. 教师及课程基本情况表

6.1 专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
汇编语言	3	3	代琪怡、霍雅琴	4
网络空间安全智能决策	2	2	彭光辉、黄海涛	5
网络服务配置与管理	3	3	彭玉兰	4
网络攻击与防御	4	4	谢彩云、王源源	4
认知域对抗与防御	4	4	钟琳、刘洁芯	6
网络安全设备配置与管理	4	4	向春玲	5
数据安全理论与实践	3	3	张虫金、罗焱	5
网络安全等级保护测评技术	3	3	唐坤剑、高艺珊	6
代码安全审计	3	3	陈文字、廖西	5
网络空间治理	2	2	杜亚军	6

6.2 本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历 毕业学校	最后学历 毕业专业	最后学历 毕业学位	研究领域	专职/ 兼职
彭光辉	男	1962-10	网络空间安全智能决策	教授	大学本科	中国人民解放军网络空间部队信息工程大学	计算机工程	学士	网络安全、大模型应用	专职
杜亚军	男	1967-02	网络空间治理	教授	研究生	西南交通大学	交通信息工程与控制	博士	人工智能、社交网络舆情	兼职
陈文字	男	1968-07	代码安全审计	教授	研究生	电子科技大学	计算机应用技术	博士	编译原理、形式语言与自动机理论、模式识别、自然语言处理	兼职

王源源	男	1984-07	网络攻击与防御	教授	研究生	电子科技大学	软件工程	硕士	智能计算、嵌入式系统、图像目标识别	专职
黄海涛	男	1987-05	网络空间安全智能决策	副教授	研究生	韩国东国大学	多媒体工学	博士	人工智能	专职
唐坤剑	男	1977-05	网络安全等级保护测评技术	副教授	研究生	武汉大学	计算机技术	硕士	网络工程、网络安全	专职
钟琳	女	1982-02	认知域对抗与防御	副教授	研究生	西南交通大学	计算机技术	硕士	计算机应用、软件工程	专职
罗焱	女	1987-03	数据安全理论与实践	其他副高级	研究生	电子科技大学	公共管理	硕士	网络安全	专职
张虫金	男	1989-11	数据安全理论与实践	其他副高级	研究生	成都信息工程大学	农业工程与信息技术	硕士	网络安全	专职
廖西	女	1990-12	代码安全审计	讲师	研究生	成都信息工程大学	农业工程与信息技术	硕士	网络安全	专职
代琪怡	女	1981-07	汇编语言	讲师	研究生	重庆理工大学	信号与信息处理	硕士	二进制安全	专职
谢彩云	女	1984-07	网络攻击与防御	讲师	研究生	湖南大学	研究生	硕士	网络安全/人工智能	专职
刘洁芯	女	1992-01	认知域对抗与防御	讲师	研究生	成都信息工程大学	农业信息化	硕士	人工智能	专职
向春玲	女	1990-03	网络安全设备配置与管理	其他中级	研究生	成都信息工程大学	物联网技术	硕士	密码应用安全、侧信道安全	专职
彭玉兰	女	1988-05	网络服务配置与管理	其他中级	研究生	西南交通大学	通信与信息系统	硕士	网络安全	专职
高艺珊	女	1996-08	网络安全等级保护	未评级	研究生	成都信息工程大学	计算机技术	硕士	网络安全	专职

			测评技术							
霍雅琴	女	1981-09	汇编语言	未评级	研究生	电子科技大学	机械电子	硕士	网络安全	专职

6.3教师及开课情况汇总表

专任教师总数	15		
具有教授（含其他正高级）职称教师数	4	比例	23.53%
具有副教授及以上（含其他副高级）职称教师数	9	比例	52.94%
具有硕士及以上学位教师数	16	比例	94.12%
具有博士学位教师数	3	比例	17.65%
35岁及以下青年教师数	5	比例	29.41%
36-55岁教师数	9	比例	52.94%
兼职/专任教师比例	2:15		
专业核心课程门数	10		
专业核心课程任课教师数	17		

7. 专业主要带头人简介

姓名	彭光辉	性别	男	专业技术职务	教授	行政职务	计算机学院常务副院长
拟承担课程	网络空间安全智能决策			现在所在单位	电子科技大学成都学院		
最后学历毕业时间、学校、专业		1982年毕业于中国人民解放军网络空间部队信息工程大学计算机工程专业					
主要研究方向		网络安全、大模型应用					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		撰写《网络数据获取与协议分析上、下》、《大数据导论》三部教材，担任《领域知识工程学》副主编。					
从事科学研究及获奖情况		(1)四川省科技进步一等奖一项、三等奖一项； (2)参与了公安部，安全部、工信部，军队，发改委多个国家重点项目的建设和多个标准的制定工作，是工信部《互联网数据中心和互联网接入服务信息安全管理系统及接口测试方法》、《互联网数据中心和互联网接入服务信息安全管理系统技术要求》、《互联网数据中心和互联网接入服务信息安全管理系统接口规范》三个技术标准的起草专家； (3)参与国家发改委国家重要信息系统可控性验证服务论证报告的编写工作； (4)参与了国家市场监管总局《网络市场监管与服务示范区创建研究》课题组工作； 近几年取得5项发明专利（一种用于 IDC 有害信息监测平台的数据分析、网络用户行为责任认定与管理系统、一种用于IDC有害信息监测平台的爬虫系统、一种基于IDC有害信息监测系统的样本训练、互联网数据中心有害信息监测系统、基于招聘信息的岗位词条构建方法）。					
近三年获得教学研究经费（万元）	6.0			近三年获得科学研究经费（万元）	115.0		
近三年给本科生授课课程及学时数	授课网络数据获取与分析、PBL课程 共计学时336			近三年指导本科毕业设计（人次）	20		
姓名	杜亚军	性别	男	专业技术职务	教授	行政职务	计算机学院

				务			院长
拟承担课程	网络空间治理			现在所在单位	西华大学		
最后学历毕业时间、学校、专业		2005年毕业于西南交通大学交通信息工程与控制专业					
主要研究方向		人工智能、社交网络舆情					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		获奖： 2021年05月被四川省人民政府评为四川省教学成果二等奖； 2014年05月被四川省人民政府评为2013年优秀教学成果； 专著与教材： 概念背景图及应用，杜亚军等著，科学出版社，2022年09月； C++语言与面向对象的设计，张兴明，杜亚军等编，重大出版社，2000年07月； 算法设计与分析，宋文，杜亚军等编，重大出版社，2000年07月。					
从事科学研究及获奖情况		(1) 主持国家自然科学基金重点/面上项目5项；主研完成国家部属八五、九五重点科技攻关项目4项，承担九五重点科技攻关项目子课题2项，主持研究省部级横向项目10余项，主持完成企业合作纵向项目40余项； (2) 2023年12月四川省人民政府科技进步，省部三等奖； (3) 2023年12月中国物流与采购联合会科技进步，省部一等奖； (4) 2024年12月中国物流与采购联合会科技进步，省部一等奖。					
近三年获得教学研究经费（万元）	0.0			近三年获得科学研究经费（万元）	50.0		
近三年给本科生授课课程及学时数	授课软件工程课程学时144			近三年指导本科毕业设计（人次）	30		
姓名	陈文字	性别	男	专业技术职务	教授	行政职务	无
拟承担课程	代码安全审计			现在所在单位	电子科技大学		
最后学历毕业时间、学校、专业		2009年毕业于电子科技大学计算机应用技术					
主要研究方向		编译原理，形式语言与自动机理论，模式识别，自然语言处理					

从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	(1) 陈文字；桑永胜；刘贵松；邱钊；神经网络在路径优化问题中的应用，电子科技大学出版社，2014（学术专著学术专著）； (2) Siying Wang; Xiaodie Li; Hong Qu; Wenyu ChenWenyu Chen；State Augmentation via Self-supervision in Offline Multi-Agent Reinforcement Learning, IEEE Transactions on Cognitive and Developmental Systems, 2023（期刊论文期刊论文）（本人标注：唯一通讯作者）； (3) Kang, Zhao; Lu, Xiao; Lu, Yiwei; Peng, Chong; Chen, WenyuChen, Wenyu; Xu, Zenglin；Structure learning with similarity preserving, Neural Networks, 2020, 129: 138-148（期刊论文期刊论文）（本人标注：共同通讯作者）； (4) Kang Zhao; Liangjian Wen; Chen WenyuChen Wenyu; Zenglin Xu；Low-rank kernel learning for graph-based clustering, Knowledge-Based Systems, 2019, 163: 510-517（期刊论文期刊论文）（本人标注：共同通讯作者）； (5) Dingyi Zeng; Li Zhou; Wanlong Liu; Hong Qu; Wenyu ChenWenyu Chen；A Simple Graph Neural Network Via Layer Sniffer, 2022 IEEE International Conference on Acoustics, Speech and Signal Processing, 香港中文大学（深圳），2022-05-22至2022-05-27（会议论文会议论文）（本人标注：唯一通讯作者）。
从事科学研究及获奖情况	(1) 国家自然科学基金委员会，联合基金项目，U22B2061，多模态数据驱动的事件表征与可解释性推理方法研究，2023-01-01 至 2026-12-31，252万元，在研，参与； (2) 国家科学技术部，国家重点研发计划，2018YFC0808304，“互联网+”煤炭安全监管监察关键技术研发与示范（课题四 子任务1 研究基于情感感知驱动的移动执法方法），2018-07 至 2021-09，30万元，结题，主持； (3) 陈文字；熊志斌；黄卫华；刘强；刘井波；具备智能感知的富文本控件制作方法，2012-7-18，中国，ZL 20081004551.5（专利）； (4) 刘贵松；陈文字；罗光春；秦科；蔡庆；李宝程；基于深度学习的移动平台烟草激光码智能识别方法及装置，2017-8-25，中国，ZL201510025849.9（专利）； (5) 康昭；陆啸；陈文字；苏元章；一种基于核保持的图像相似性度量方法，2022-05-03，中国，ZL201910085067.2（专利）；

		(6) 屈鸿; 王晓斌; 杨媛静; 陈文字; 刘贵松 ; 一种基于拟退火算法的三维人脸识别方法, 2013-12-18, 中国, ZL201210109651.5 (专利); (7) 王晓斌; 屈鸿; 孙明; 陈文字; 陈常乐 ; 一种基于本体的电子商务推荐方法, 2018-8-3, 中国, ZL201510493439.7 (专利); (8) 刘贵松; 邱钊; 谢娟; 张浩; 屈鸿; 陈文字 ; 一种应用于GPS的快速K最短路径规划方法, 2015-1-21, 中国, ZL201310400749.0 (专利); (9) 刘贵松; 屈鸿; 邱钊; 蔡庆; 解修蕊; 陈文字; 王晓彬 ; 基于图像扫描的植物叶片特征分析系统, 2013-5-1, 中国, CN201310061389.6 (专利);					
近三年获得教学研究经费(万元)	30.0		近三年获得科学研究经费(万元)	300.0			
近三年给本科生授课课程及学时数	程序设计基础, 数据结构与算法, C++程序设计, 编译原理, 共计课时312学时		近三年指导本科毕业设计(人次)	18			
姓名	彭玉兰	性别	女	专业技术职务	其他中级	行政职务	信息安全专业负责人
拟承担课程	网络服务配置与管理		现在所在单位	电子科技大学成都学院			
最后学历毕业时间、学校、专业	2014年毕业于西南交通大学通信与信息系统专业						
主要研究方向	网络安全						
从事教育教学改革研究与获奖情况(含教改项目、研究论文、慕课、教材等)	2024年4月教学研究与教学改革项目《网络数据获取与协议分析》教学方法与实践内容改革立项。 2022年9月25日在现代信息科技的第6卷第18期发表论文《基于GNS3+Wireshark 的网络协议分析实验教学改革》。 2022年校级教学改革类项目《新工科背景下网络协议分析课程改革与探索》结项。						
从事科学研究及获奖情况	2025年5月在电子科技大学成都学院发表文章 基于msfvenom的蜜罐反制方法研究						
近三年获得教学研究经费(万元)	0.0		近三年获得科学研究经费(万元)	0.0			
近三年给本科生授课课程	授课网络数据获取与分析、PBL课程 共计学时1248		近三年指导本科毕业设	46			

程及学时数				计（人次）			
姓名	向春玲	性别	女	专业技术职务	其他中级	行政职务	无
拟承担课程	网络安全设备配置与管理			现在所在单位	电子科技大学成都学院		
最后学历毕业时间、学校、专业	2016年毕业于成都信息工程大学物联网技术专业						
主要研究方向	密码应用安全、侧信道安全、物联网安全						
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	无						
从事科学研究及获奖情况	(1) 四川省科技进步奖二等奖； (2) 参与《PLC控制系统及PLC控制器密码应用技术规范》、《TEE的密码安全管理框架与接口规范标准》标准制定； (3) 授权发明专利2项（针对SM2解密算法的能量分析检测方法、一种针对SM3密码算法消息扩展的侧信道分析攻击的方法）、授权实用新型专利2项（一种针对USBKey的能量迹提取仪、一种针对CPU式智能卡的能量迹提取仪）； (4) 参与十三五密码基金、国密局商检中心、企事业单位等密码产品检测工具、密评检测工具开发十余项；参与密码应用系统安全测评数项。						
近三年获得教学研究经费（万元）	0.0			近三年获得科学研究经费（万元）	0.0		
近三年给本科生授课课程及学时数	计算机基础、C语言、PBL6/7项目实践共计学时336			近三年指导本科毕业设计（人次）	16		
姓名	张虫金	性别	男	专业技术职务	其他副高级	行政职务	网络工程专业负责人
拟承担课程	数据安全理论与实践			现在所在单位	电子科技大学成都学院		
最后学历毕业时间、学校、专业	2015年毕业于成都信息工程大学农业工程与信息技术专业						
主要研究方向	网络安全						
从事教育教学改革研究	(1) 教育部协同育人-新工科视域下基于AI赋能的网络工程专业教学路径探						

及获奖情况（含教改项目、研究论文、慕课、教材等）	究，主持，2024年9月立项； （2）教育部就业育人： 电子科技大学成都学院 -成都国信安信息产业基地有限公司就业实习基地项目，主持。2024年6月立项； （3）校级教改-基于“产、赛、学”融合AI大模型的Web前端开发课程改革，主持，2024年4月立项； （4）校级教改-基于 区块链 技术的智能粮油溯源系统设计与研究，主持，2024年10月结项。 （5）“”新互联网“”时代背景下高校网络工程专业建设的探索与研究，《医学研究》，排名第一，2021年10月； （6）基于“产、赛、学”融合AI大模型的Web前端课程改革，《电子科技大学成都学院学报》，排名第一，2024年10月。 （7）新工科视域下基于AI赋能的网络工程专业教学路径探究，电子科技大学成都学院学报，排名第一，2025年4月。		
从事科学研究及获奖情况	（1）用于物联网的RPL节能负载均衡方法，西南大学学报（自然科学版），CSCD/ 北大 核心，排名第一，2022年9月； （2）基于三层B/S模式的分布式系统设计，计算机产品与流通，独立，2020年10月； （3）基于区块链技术的食用农产品溯源系统研究，电子科技大学成都学院学报，排名第一，2023年4月； SSM框架在web开发中的设计，电子科技大学成都学院学报，排名第一，2023年10月； （4）浅谈 校园网络安全 防范措施，电子科技大学成都学院学报，排名第一，2024年01月； （5）基于区块链与物联网的智能粮油溯源系统研究，时代论坛，排名第一，2024年8月 （6）发明专利-一种台式计算机主机移动式自动散热除尘装置，独立发明，2023年11月授权。		
近三年获得教学研究经费（万元）	0.2	近三年获得科学研究经费（万元）	5.0
近三年给本科生授课课程及学时数	“授课计算机网络、网络空间安全导论、区块链编程、区块链项目实战、PBL3/7项目实战、PBL4/7项目实践、PBL1/7项目实践 共计学时672”		
	近三年指导本科毕业设计（人次）	92	

8. 教学条件情况表

可用于该专业的教学实验设备总价值（万元）	118.0	可用于该专业的教学实验设备数量（千元以上）	55（台/件）
开办经费及来源	100万/学校拨款		
生均年教学日常运行支出（元）	1500.0		
实践教学基地（个）	1		
教学条件建设规划及保障措施	一、教学条件建设规划 1、硬件设施建设 短期内，投入资金购置高性能计算机、服务器、网络设备等，搭建网络安全实验室，模拟真实网络环境，满足学生实践需求。 中长期，逐步升级设备，引入云计算、大数据等前沿技术平台，建设智慧教室，实现线上线下混合式教学。 2、软件资源配备 订购专业网络安全软件、数据库系统，保障学生学习实践；引入正版教材、在线课程资源，拓宽学生知识面。 自主开发教学案例库、实验指导书，结合行业实际，增强教学针对性。 3、师资队伍建设 引进网络安全领域专家、工程师，充实教师队伍；选派教师参加学术交流、企业挂职锻炼，提升专业水平。 定期组织教师培训，更新知识体系，培养“双师型”教师。 二、保障措施 1、资金保障 设立专项经费，用于设备采购、软件更新、师资培养；积极争取政府、企业资助，拓宽资金来源。 2、管理保障 建立健全设备管理制度，确保实验室高效运行；制定教学资源使用规范，保障资源合理利用。 3、合作保障 加强与企业合作，共建实习基地，为学生提供实践机会；与高校、科研机构合作，共享资源，开展学术交流。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
计算机	G2030/华硕P8H61/4G/ST500G/PHS液晶20寸	35	2015	87.5
服务器硬盘(Z)	SAS 600G(2.5/10K转)	10	2013	18.72
机架式服务器(Z)	R620(E5-2650*2/64G/SAS/600G*2iDRAC/H310/滑轨)	10	2013	331.0
云终端(Z)	YTv901	10	2013	16.0
网络存储设备(Z)	DELL 3600I(SAS2T*6)	1	2013	44.0
上网行为网关	Sangfor SG3400-H	1	2013	34.84
核心网络交换机(Z)	Cisco C3750X-24T-S	1	2013	17.2
接入网络交换机(Z)	Cisco SLM2024T-CN	10	2013	25.0
云计算节点服务器(Z)	ELL R620	10	2013	332.0
计算机组成实验系统Z	EL-JY-II(16位)	10	2018	22.5
网络安全交换机	华为1730S-S24T4S-A1	10	2021	16.5
计算机	联想天启i5-12500 8G 1T	35	2023	128.45

9. 申请增设专业的理由和基础

申请增设专业的理由和基础

（应包括申请增设专业的主要理由、支撑该专业发展的学科基础、学校专业发展规划、与现有专业的区分度、专业名称的规范性等方面的内容）

（一）主要理由

1. 国家安全与战略发展的迫切需求

网络空间已成为国家第五疆域，关键基础设施（如能源、金融、交通）的数字化转型使安全威胁直接关联国家安全。据《2024 中国网络安全产业白皮书》统计，我国每年因网络攻击造成的经济损失超千亿元，亟需专业人才构建主动防御体系。2015 年，国务院将“网络空间安全”列为一级学科，并提出“建设网络强国”的目标。增设本科专业是落实国家战略的基础性举措，为国家培养急需的网络安全人才。

2. 人才缺口巨大，市场需求迫切

供需严重失衡：据全球统计，网络安全人才缺口达数百万，我国缺口占比居高不下，本科专业设置可系统化培养人才，缓解行业“用人荒”。

政策法规推动：《数据安全法》《个人信息保护法》《密码法》等法规的实施，要求企业加强数据安全与合规治理，进一步扩大了人才需求。

复合型能力要求：网络安全涉及计算机科学、密码学、法律、管理学等多学科，需通过本科教育整合知识体系，培养跨领域能力。

3. 数字经济转型的技术支撑

新技术场景的安全挑战：物联网、人工智能、量子计算等领域催生出新型攻击面。例如，5G 网络切片技术可能引发跨域攻击，智能汽车的安全漏洞可能危及生命。传统安全人才的知识体系难以覆盖这些场景。

安全左移趋势：DevOps 与 DevSecOps 模式要求安全人员具备全生命周期防护能力。本科专业可设计“安全即代码”课程，培养具备开发-安全双重视角的复合型人才。

4. 教育体系的结构性补位

学科交叉性缺失：现有计算机专业偏重算法与系统设计，安全课程多作为选修模块，导致人才缺乏密码学、安全协议设计、代码安全审计、数据安全隐私保护等纵深能力。独立专业可构建“攻防对抗-漏洞挖掘-应急响应”的完整培养链

条。

产教融合路径：参照美国马里兰帕克分校模式，通过校企共建实验室（如工业控制系统安全靶场），实现“理论-实战”无缝衔接。华为等企业已提出“网络安全人才联盟”，反映行业对专业对口人才的需求。

5. 职业生态的规范化发展需求

职称评审与职业认证：北京市等多地区已增设网络空间安全职称评审专业，涵盖网络与系统安全、数据安全等方向，为从业者提供职业晋升路径。本科专业作为职称评审的学历基础，可吸引更多人才进入该领域。

行业认可与规范：通过统一的专业培养标准（如《网络空间安全专业职称申报标准条件》），确保人才技能与行业需求对接，提升职业含金量。

（二）支撑该专业发展的学科基础

结合学院现有基础增设网络空间安全专业，具有学科生态优势、产教融合优势、竞赛创新优势三重核心基础。

一、学科生态：现有专业形成强力支撑

信息安全专业协同：密码学基础、安全协议分析等课程可直接移植，构建新专业“安全基础模块”。

计算机科学与技术/软件工程专业奠基：四川省一流本科专业建设经验可直接复制，如“项目驱动教学”“企业案例库”等模式。

人工智能/大数据交叉创新：基于人工智能实验班的《深度学习》课程，增设《AI 安全对抗》前沿方向。

大数据专业的隐私计算研究成果，可转化为《数据泄露防护》特色课程。

二、产教融合：校企协同深度赋能

拟新设立的网络空间安全专业，在本系兄弟专业“信息安全”所合作的生态企业助力下，将全方位覆盖网络空间安全行业。目前，我们合作的企业包括奇安信科技集团股份有限公司、成都国信安信息产业基地有限公司、成都数字奇安科技有限公司、工业信息安全（四川）创新中心有限公司、安恒科技有限公司。这些企业能够全面支持“网络空间安全”专业的实践与应用场景，还能针对该专业面向相关企业的需求，提供驱动力与方向指引。目前，我们已经开展的与该专业相关的校企合作项目如下：

（1）2021 年，奇安信科技集团股份有限公司提供“奇安信网神网络安全实

训系统”，助力本系网络工程、信息安全方向的学生提升网络安全技能。

(2) 2025 年，与亚信安全合作参与第 12 届世界运动会网络安保项目，20 名学生参与其中。

(3) 2023 年，与安恒公司合作参与第 31 届世界大学生运动会网络安保项目，参与学生人数为 32 人。

(4) 2022 年，与中国电子科技集团有限公司（30 所）合作，安排骨干教师为巴基斯坦技术人员开展为期 22 天的网络安全技能提升培训。

头部企业战略合作

奇安信参与共建的“网络安全实验室”可直接服务新专业，提供实验平台。

工业信息安全创新中心合作开发“工业互联网安全”方向，对接四川省智能制造需求。

实训资源升级

依托 360 企业安全实训基地，建设“网络安全应急响应”实战平台。

三、竞赛创新：特色培养体系成熟

竞赛成果迁移

中国大学生计算机设计大赛获奖作品转化为课程设计案例。

“挑战杯”省级金奖项目（如 APT 攻击链分析）升级为《高级威胁检测》课程模块。

特色班经验复用

网络安全实验班的“红蓝对抗”模式扩展为专业核心实践环节。

创智班“双创导师制”引入安全创业项目孵化。

（三）学校专业发展规划

1、专业建设目标

总体定位

建成服务国家战略、对接产业需求、特色鲜明的网络空间安全专业，形成“技术+法律+管理”复合型高级应用型人才的培养体系，打造区域或行业内有影响力的特色专业。

阶段目标

1 - 2 年：完成专业申报与基础建设；

3 - 4 年：形成稳定教学团队与特色课程；

5 年：通过专业认证，输出高质量就业人才。			
2、主要建设内容			
（1）人才培养体系建设			
专业课程体系			
核心课程：汇编语言、网络攻击与防御、认知域对抗与防御、网络安全设备配置与管理、数据安全理论与实践、网络安全等级保护测评技术、代码安全审计、网络服务配置与管理、网络空间治理、网络空间安全智能决策。			
教学模式			
校企协同：企业导师参与授课（如“双师课堂”），共建实战课程。			
竞赛驱动：以 CTF 竞赛、漏洞挖掘比赛替代部分课程考核。			
（2）实验室教学平台建设			
基础实验室：网络攻防靶场、密码学实验平台、恶意代码分析环境。			
特色实验室：工业控制系统安全实验室。			
实习基地：签约网络安全企业作为实习基地。			
（3）师资能力提升			
引进与培养：1）5 年内引进或培养网络安全领域高级职称人员。2）专业教师具备行业认证或企业实践经历。			
校企共育：实施“双导师制”，聘请校外网络空间安全专家参与毕业设计和课程设计。			
（4）科研与社会服务			
科研方向： 聚焦密码应用安全、AI 安全等前沿领域，申报科研项目。			
社会服务： 成立“网络安全服务中心”，提供漏洞扫描、应急响应等服务。			
（四）与现有专业的区分度			
电子科技大学成都学院现有相关本科专业信息安全和网络工程，其中网络工程 2005 年开设，信息安全 2017 年开设，拟申报的网络空间安全作为该两个专业的补充主要培养网络安全和通信安全方面的人才，并形成数据安全、工业安全、网络安全三个大类方向的闭环，具体如下表 9.1：			
表 9.1 专业布局和产业方向			
专业	专业布局方向	核心课程	备注
网络工程	产业方向：智慧安全服务 技能方向：工控安全	区块链基础、工控协议安全	现有拟优化

信息安全	产业方向：智能安全预警 技能方向：全生命周期的数据安全	密码学、电子取证、大数据安全	现有拟优化
网络空间安全	产业方向：互联网+安全 技能方向：网络安全和通信安全	网络攻防、计算机等级保护、计算机病毒	拟新增

（五）专业名称的规范性

该专业名称符合国际通用标准（Cybersecurity）与国内权威规范：2015 年被列为国家一级学科（代码 083900），本科专业目录明确归属计算机类（代码 080911TK），与《网络安全法》《数据安全法》等法规表述一致，体现法律与政策层面的高度认可。

名称严格区分于相近专业：与“信息安全”相比，其保护范围扩展至网络基础设施、通信协议等全域空间，技术手段侧重攻防对抗；与“计算机科学”“网络工程”则聚焦安全防护而非系统开发或网络运维。

名称的学术严谨性支撑其行业认可度：直接对应 327 万人才缺口，与 CISSP、OSCP 等国际认证对接，助力学生高薪就业。名称规范避免了专业混淆，为政策落地、学科建设及国际化发展提供标准化依据。

10. 校内专业设置评议专家组意见表

校内专业设置评议专家组意见表

总体判断拟开设专业是否可行	☒ 是 ☐ 否
理由： 经对我校申请增设的“网络空间安全（080911TK）”本科专业进行全面、细致评议，专家组认为： 一、专业定位准确，适应国家安全与战略发展需求。网络空间作为国家第五疆域，关键基础设施（如能源、金融、交通）的数字化转型使安全威胁直接关联国家安全。网络空间安全作为国家科技发展规划的重点领域，对国防建设和国民经济发展具有重要意义。成都与重庆共同构建有国家网络安全产业园区（成渝地区），成都地区作为我国网络安全的核心基地，汇聚了众多网络安全企业，对专业人才的需求迫切且规模庞大。该专业的设置旨在满足数字化经济及信息化建设中网络空间安全专业人才的需求，定位准确，具有广阔的发展前景。 二、学科基础扎实，教学经验丰富。我校计算机学院自 2005 年起开始招收网络工程专业本科生，自 2017 年起开始招收信息安全专业本科生，历年生源稳定，专业对口就业率持续保持高位，同时，行业对我校网络工程和信息安全专业毕业生的评价一直较高，这充分证明我校在网络及网络安全领域的教学实力和就业竞争力。 三、专业规划全面系统，教学条件扎实。学校现有信息安全与网络工程专业，分别聚焦数据安全与工控安全方向，但缺乏对网络安全与通信安全领域的系统性覆盖。新增网络空间安全专业可填补这一空白，形成“数据安全—工业安全—网络安全”三位一体的学科闭环；同时，我校已与奇安信、工业信息安全创新中心、360 等多家优质企业建立战略合作关系，为学生的学习、实践、就业提供了优越的条件。 四、师资队伍雄厚，教学科研实力强。专业组建了以行业专家、兼具丰富实践经验和扎实理论功底的“双师型”教师、硕博士高学历理论教师为核心的师资队伍，结构合理、教学科研经验丰富，能够胜任新专业的教学和科研工作。 综上所述，“网络空间安全（080911TK）”专业符合我校的办学定位和战略规划，具有较好的申报基础和条件。专家组一致同意该专业进行申报。	

拟招生人数与人才需求预测是否匹配		√是 □否
本专业开设的基本条件是否符合教学质量国家标准	教师队伍	√是 □否
	实践条件	√是 □否
	经费保障	√是 □否
签字： 张四喜 李 磊 杨 振 刚		